UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 09/765,907 | 01/19/2001 | Stephen M. Trimberger | X-714 US | 9367 |

24309 7590 02/09/2007

XILINX, INC
ATTN: LEGAL DEPARTMENT
2100 LOGIC DR
SAN JOSE, CA 95124

| EXAMINER | |
|---|---|
| COLIN, CARL G | |
| ART UNIT | PAPER NUMBER |
| 2136 | |

| SHORTENED STATUTORY PERIOD OF RESPONSE | MAIL DATE | DELIVERY MODE |
|---|---|---|
| 3 MONTHS | 02/09/2007 | PAPER |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 09/765,907 | TRIMBERGER, STEPHEN M. | |
| | Examiner | Art Unit | |
| | Carl Colin | 2136 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *13 November 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1-4,7,12,13,15,21 and 44* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-4, 7, 12-13, 15, 21, and 44* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

## DETAILED ACTION

### *Response to Arguments*

1. In response to communications filed on 11/13/2006, applicant amends claims 1 and 12, and adds claim 44. The following claims 1-4, 7, 12-13, 15, 21, and 44 are presented for examination.

2. Applicant's arguments, pages 5-8, filed on 11/13/2006, with respect to the rejection of claims 1 and 12 have been fully considered, but they are moot in view of a new ground of rejection. Claims 1 and 12 have been amended to overcome the 112th rejection. By canceling the added limitations, claims 1 and 12 are presented with the same limitation before the Final Rejection. Since the final rejection has not been overcome by Applicant, as indicated by Examiner in the last phone interview, the IBM Technical Disclosure Bulletin reference will still be applicable to the claim rejection as shown in the last Final rejection. The response to arguments in the last Final rejection is incorporated herein by reference. Claim 44 has been added. In response to Applicant's arguments that Mo's reference suggests a single oscillator, it is noted that the independent claims do not explicitly recite that the first oscillator and the second oscillator are different from each other. Using one or two oscillators does not patentably distinguish the claimed invention as claimed.

### *Claim Rejections - 35 USC § 103*

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

**Claims 1-4, 7, 12-13, 15, 21, and 44** are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 5,970,142 to **Erickson** in view of IBM Technical Disclosure Bulletin "Integrated Circuit Compatible Random Number Generator", April 1998, Volume 30, Issue Number 11; pages 333-335.

**As per claim 1, Erickson** discloses a method of securing communication of configuration data between a field programmable gate array (FPGA) and an external storage device comprising, the method comprising: a plurality of configurable logic elements within the FPGA being programmable with configuration data to implement a desired circuit design, for example (see column 3, lines 5-21); transmitting encrypted configuration data from the storage device to the FPGA, for example (see column 3, lines 34-36); and a decryption circuit coupled to received encrypted configuration data, the decryption circuit configured to decrypt the encrypted configuration data in the FPGA using the fingerprint as a decryption key to extract the configuration data, for example (see column 3, lines 34-42). **Erickson** discloses a security circuit comprising a key generator for generating a key (column 2, lines 30-31) and the security

circuit also comprises a security initialization circuit for generating initialization data to be used for encryption/decryption (column 4, lines 44-65) that meets the recitation of fingerprint element for generating fingerprint representing inherent manufacturing process variations unique to the FPGA. **Erickson** does not explicitly disclose a random number generator comprises oscillators and measuring the oscillations and combining them to generate the key. IBM Technical Disclosure Bulletin discloses generating random binary numbers for use to supply inputs for encryption/decryption function that can be implemented with standard logic circuits with high statistical quality by generating the values from oscillators (pages 333-335), the random generator circuit comprises oscillators and sensing circuit for counting the number of oscillations of a first oscillator and a second oscillator during a predetermined time interval (see bottom of page 334). One of the advantages of this random number generator to those known in the art, as stated this disclosure, is that in contrast to other generators known in the art that produce non-deterministic random values, this technique can be adapted to modern digital VLSI technologies by counting down the output of oscillators at a desired sampling frequency and generating a ratio between the oscillators to be used as the fingerprint that also meets the recitation of measuring and combining the propagation delays to be used as the fingerprint (page 334). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of key generation of **Erickson** to apply the concept of random number generator of the IBM Technical Disclosure Bulletin of measuring propagation delays and combining the propagation delays to generate the fingerprint as taught in IBM Technical Disclosure Bulletin because this technique provides a way of generating true random binary numbers with high statistical quality and using values from oscillators as described in the

disclosure would provide a further advantage that the technique can be adapted to modern digital VLSI technologies. The motivation to do so is given in the IBM Technical Disclosure who teaches: with a high quality random number generator, it is extremely unlikely that future or past results can be predicted; therefore, the chance of guessing the key from the security circuit is greatly reduced. In addition to generating true random binary numbers with high statistical quality, generating the values from at least two oscillators can prevent biased outputs since this technique provides the ability to vary frequencies and combining the frequencies to avoid biased outputs.

**As per claim 2,** the references as combined above disclose the claimed method of claim 1. **Erikson** further discloses the limitation configuring the FPGA using configuration data, for example (see column 3, lines 39-42).

**As per claim 3,** the references as combined above disclose the claimed method of claim 2. **Erikson** further discloses the limitation of further comprising: transmitting the fingerprint from the FPGA to an encryption circuit, for example (see column 3, lines 31-32); encrypting the configuration data using the fingerprint as an encryption key, for example (see column 3, lines 30-35); and storing the encrypted configuration data in the storage device, for example (see column 3, lines 15-18).

**As per claim 4,** the references as combined above disclose the claimed method of claim 1. **Erikson** further discloses the limitation of wherein the fingerprint generated during power-up of the FPGA, for example (see column 3, lines 25-30).

**As per claim 7,** the references as combined above disclose the claimed method of claim 1. IBM Technical Disclosure Bulletin further discloses wherein the first and second oscillators comprise configurable logic blocks (see bottom page 333 and page 33 4, lines 7-10). Claim 21 is rejected on the same rationale as the rejection of claim 1.

**As per claim 12, Erickson** discloses an FPGA comprising: a plurality of configurable logic elements within the FPGA being programmable with configuration data to implement a desired circuit design, for example (see column 3, lines 5-21); transmitting encrypted configuration data from the storage device to the FPGA, for example (see column 3, lines 34-36); and a decryption circuit coupled to received encrypted configuration data, the decryption circuit configured to decrypt the encrypted configuration data in the FPGA using the fingerprint as a decryption key to extract the configuration data, for example (see column 3, lines 34-42). **Erickson** discloses a security circuit comprising a key generator for generating a key (column 2, lines 30-31) and the security circuit also comprises a security initialization circuit for generating initialization data to be used for encryption/decryption (column 4, lines 44-65) that meets the recitation of fingerprint element for generating fingerprint representing inherent manufacturing process variations unique to the FPGA. **Erickson** does not explicitly disclose a random number generator comprises oscillators and measuring the oscillations and combining them to generate

the key. IBM Technical Disclosure Bulletin discloses generating random binary numbers for use to supply inputs for encryption/decryption function that can be implemented with standard logic circuits with high statistical quality by generating the values from oscillators (pages 333-335), the random generator circuit comprises oscillators and sensing circuit for counting the number of oscillations of a first oscillator and a second oscillator during a predetermined time interval (see bottom of page 334) that meets the recitation of means for counting a first number of oscillations of the first oscillator and counting a second number of oscillations of the second oscillator during a predetermined time interval and means for generating a fingerprint as a ratio between the number of oscillations. One of the advantages of this random number generator to those known in the art, as stated this disclosure, is that in contrast to other generators known in the art that produce non-deterministic random values, this technique can be adapted to modern digital VLSI technologies by counting down the output of oscillators at a desired sampling frequency and generating a ratio between the oscillators to be used as the fingerprint that also meets the recitation of measuring and combining the propagation delays to be used as the fingerprint (page 334). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of key generation of **Erickson** to apply the concept of random number generator of the IBM Technical Disclosure Bulletin of measuring propagation delays and combining the propagation delays to generate the fingerprint as taught in IBM Technical Disclosure Bulletin because this technique provides a way of generating true random binary numbers with high statistical quality and using values from oscillators as described in the disclosure would provide a further advantage that the technique can be adapted to modern digital VLSI technologies. The motivation to do so is given in the IBM Technical Disclosure who

teaches: with a high quality random number generator, it is extremely unlikely that future or past results can be predicted; therefore, the chance of guessing the key from the security circuit is greatly reduced. In addition to generating true random binary numbers with high statistical quality, generating the values from a first oscillator and a second oscillator can prevent biased outputs since this technique provides the ability to vary frequencies and combining the frequencies to avoid biased outputs.

**As per claim 13,** the references as combined above disclose the claimed FPGA of claim 12. **Erikson** further discloses a configuration circuit for configuring the FPGA using configuration data, for example (see column 3, lines 39-42).

**As per claim 15,** the references as combined above disclose the claimed FPGA of claim 12. **Erikson** further discloses transmitting the fingerprint from the FPGA to an encryption circuit, for example (see column 3, lines 31-32); encrypting the configuration data using the fingerprint as an encryption key, for example (see column 3, lines 30-35); and storing the encrypted configuration data in the storage device, for example (see column 3, lines 15-18).

**As per claim 21,** the references as combined above disclose the claimed FPGA of claim 12. IBM Technical Disclosure Bulletin further discloses wherein the first and second oscillators comprise configurable logic blocks (see bottom page 333 and page 33 4, lines 7-10). Claim 21 is rejected on the same rationale as the rejection of claim 12.

**As per claim 44,** the references as combined above disclose the claimed method of claim 1. IBM Technical Disclosure Bulletin further discloses using the ratio of the jitter oscillator frequency to the sampling oscillator frequency (see page 334 more specifically the bottom of the page). As interpreted by the Examiner the ratio is the quotient of one value dividing by the other. As disclosed in the reference, the ratio is taken between the value of the oscillator that is set to the desired frequency (sampling) and the other oscillator (jitter oscillator) (bottom of page 334). This meets the recitation of generating the ratio is obtained by dividing the first number of oscillations by the second number of oscillations.

***Conclusion***

4. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

4.1 Any inquiry concerning this communication or earlier communications from the examiner should be directed to Carl Colin whose telephone number is 571-272-3862. The examiner can normally be reached on Monday through Thursday, 8:00-6:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser G. Moazzami can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

cc

Carl Colin
Patent Examiner
February 3, 2007

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

2/5/07